LN-4

複数サービスが利用する個人情報に関する管理方式の検討
Personal Information Manager referred by Multiple Services

出沢 信雄† 小久保 勝敏† 岩城 修†
Nobuo Idezawa Katsutoshi Kokubo Osamu Iwaki

1．はじめに

近年、個人情報を電子化し活用することでサービスの高度化を図る動きがおきている。加えて、昨今のサービス集約化の流れにより、各種情報を集約し活用することが検討されており、米マイクロソフト社の.Net Passport[1]や Liberty Alliance Project [2]など集約した個人情報に対して複数のサービスがその情報を活用するといったシーンが増えつつある。その反面、行政、民間を問わず管理している個人情報が流出する事件がこの数年の間に大幅に増加している[3]。特に電子化された個人情報は、一旦情報が漏洩してしまうと短期間のうちに拡散してしまう恐れがあり、その結果、情報提供者である情報主体が様々な被害をうける可能性がある。

本稿ではこうした状況において、電子化された個人情報を集約管理し、複数のサービス提供者が個人情報を活用するようなシステムに対して、より安全性の高い個人情報管理方式を提案する。

2．個人情報活用システムの問題点

個人情報が公の場に公開されると精神的被害や金銭的被害といった実害が発生する恐れがあるため、細心の注意を払う必要がある。こうした背景から個人情報活用システムでの問題として、管理している個人情報の漏洩がある。その主な漏洩原因としては技術的な原因と人的な原因といった2つ原因がある。

2.1 技術的原因

技術的原因に挙げられるものは主に3つで、個人情報管理サーバに対し情報参照権利のあるユーザになりすまし情報を入手するもの、セキュリティホールをついて不正アクセスするもの、ネットワーク上での盗聴がある。盗聴については SSL での暗号化など有効な対策がとられているが、なりすましと不正アクセスについては十分な対策がとれているところは少ない。

2.2 人的原因

人的原因に挙げられるものは主に2つで、サポートセンタなどに第三者が情報主体になりすまして ID とパスワードを不正に聞き出すといったソーシャルエンジニアリングと悪意を持ったシステム管理者が個人情報を故意に漏洩することが挙げられる。このうちソーシャルエンジニアリングについては、情報主体へのダブルオプトインや PKI による本人認証が有効な対策としてとられているが、システム管理者による個人情報の故意の漏洩については、システム管理者に対する倫理教育など人的対策はあるものの技術的な対策はあまりとられていない。

† 株式会社 NTT データ 技術開発本部

3．個人情報の定義

個人情報保護法制化専門委員会による個人情報保護法案によると個人情報の定義は、「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるものをいう」とされている[4]。その典型的な例として、氏名、住所、性別、生年月日の情報の集合があげられる。いわゆる基本4情報と呼ばれるもので、住民基本台帳法ではこの4情報が揃うと個人を識別可能であるとしている[5]。だが、逆を返すと特定の個人を識別できないような情報は個人情報と見なされない。しかし、個人情報保護法案において個人情報は「他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む」とも定義されているように、いくつかの情報を組合せた場合、個人情報でなかった情報が一転して個人情報となってしまう場合があるため注意が必要となる。

4．個人情報漏洩に対する現状の対策と問題点

2章で述べた個人情報漏洩の原因のうち、現状で十分対策がとれていない問題として、なりすまし、不正アクセスやシステム管理者による故意の漏洩をあげたが、それらについての対策を検討する。なお、本稿ではサービス提供者が得ることのできる電子的な個人情報の漏洩を防ぐ点を中心に検討している。

4.1 匿名化状態で個人情報を活用する仕組みとその問題

個人情報を活用するサービスにおいて、全ての個人情報を活用する場合のみならず、一部の情報のみで十分活用できる場合も存在する。その際、活用する情報だけにフォーカスすると個人情報の定義から外れる場合もある。そこで、個人情報を個人と特定できない情報に分別してそれぞれを分散管理し、サービス提供者には匿名化した情報のみを提示するといった対策が有効であると考えられる。この対策により、たとえ一つのサーバに対して不正アクセスがあったとしても、情報が個人を特定できないように分別されているため、その情報だけでは個人を特定できない。これにより個人情報の漏洩を防ぐことができると考えられる。

しかし、匿名化した個人情報であっても他の情報と組合せると個人情報となりうる可能性がある[6]。例えば、A氏の住所の一部と勤務先があるホームページに掲載されたとすると、それに関連する情報をインターネットで調べたり、名簿屋から購入した情報や住民基本台帳などで得た情報を組合せたりすることで A 氏を特定し、個人情報が入手される可能性がある。よって、たとえ匿名化した情報であっても、複製や二次利用を防ぐ仕組みが必要である。

4.2 DRMを用いた仕組みとその問題

電子化された個人情報はデジタルコンテンツの一つと見なすことができる。そこで、個人情報の複製や二次流通を防ぐ仕組みとしては DRM[7]を用いることが有効だと言える。DRM を活用することで、権限を持った者だけが専用ビュアーのみで個人情報を参照することができ、その一方でたとえシステム管理者であったとしても権限を持っていなければ個人情報を参照することが困難となる。しかし、個人情報を参照する権利を持つものが故意に個人情報を漏洩をした場合、その行動を防ぐことができないといった問題がある。DRM の一部である電子透かしを利用すれば漏洩した人間を特定することができるため、心理的な防衛策にはなりうるがこれは事後対策にすぎない。この問題への事前対策の一案としては、提供する個人情報を匿名化し、万が一情報が漏洩したとしても個人を特定できないようにすることがある。

5. 方式

5.1 提案する方式

提案する方式の一連の利用フローを考えると、大きく分けて個人情報の登録、管理と個人情報の提供の２つに分けることができる。4 章での検討より、前者の対策としては、なりすましや不正アクセスへの対策として有効な匿名化情報の提供が、後者の対策としては情報の参照制限が可能となる DRM の活用が有効であると言える。また、それぞれの対策における問題については、もう一方の対策が問題の解決策の一つとなりうるため、お互いが補完しあうことでより有効な管理方式となる。

5.2 システム構成

提案するシステム構成は、個人情報分散管理サーバ、DRM サーバ、サービス提供アプリケーションがネットワーク上でそれぞれ結ばれているシステムである。(図１)

なおここで、情報主体、個人情報管理サーバ、DRM サーバ、サービス提供 AP のそれぞれを結ぶネットワーク間でのセキュリティと各サーバに対するセキュリティは確保されていると想定する。

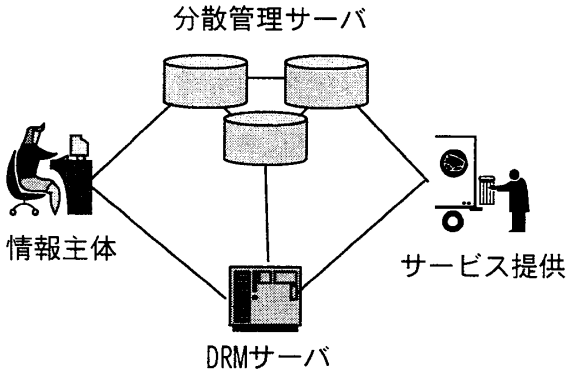

図１：システム構成図

5.3 利用フロー

本システムの利用フローを以下に示す。

（１） 個人情報の登録・管理

情報主体は、まず個人情報を管理している分散管理サーバにアクセスし、自分の個人情報を登録する。なお、登録時に個人情報を活用するサービス提供者の詳細とそれぞれのサービスにおいて活用される情報の種類について確認する。分散管理サーバは送信された情報を個人が特定できないように分別し管理する。

（２） 情報の提供

(2-1) 情報利用許可請求

サービス提供者は必要とする個人情報の利用許可を DRM サーバに要求する。その際に DRM サーバは要求者が個人情報を利用する権利を持った者であるかどうかの認証を行う。

(2-2) 承認

DRM サーバは、サービス提供者から情報開示請求があったことを情報主体に通知し、情報主体からの同意を得る。

(2-3) 情報送信

DRM サーバは開示する情報をサービス提供者の持つ公開鍵を使って暗号化し、そのデータをサービス提供者に送信する。

(2-4) 情報の参照

サービス提供者は暗号化された情報に対し、専用ビュアーと自身の持つ秘密鍵を用いて情報を復号化し、情報を参照し利用する。

6. 今後の課題

今後の課題として今回提案した個人情報管理方式の実装がある。その中でも、OS やハードに対する機種依存性やシステムの運用面での検討を中心に行っていく必要がある。特に本方式では DRM を用いるため専用リーダが必要となり、専用リーダの機種依存や情報提供アプリケーションとの親和性についての対策を検討する必要がある。

7. まとめ

本稿では、複数のサービス提供者が個人情報管理サーバにアクセスし、必要な情報を参照、活用するようなシステムにおいて、現状のシステムの問題点を指摘し、より有効な個人情報漏洩対策を施した個人情報管理方式を提案した。今後は、提案システムの実装における問題点についての検討を行っていく予定である。

参考文献

[1] .Net Passport : http://www.passport.com/
[2] Liberty Alliance Project : http://www.projectliberty.org/
[3] http://www.npa.go.jp/hightech/notice/privacy.htm
[4] 個人情報の保護に関する法律案 http://www.kantei.go.jp/jp/it/privacy/houseika/houritsuan/pdfs/327houan.pdf
[5] 住民基本台帳法 第 30 条の 29～第 30 条の 43 http://www.houko.com/00/01/S42/081.HTM
[6] 本村,橋本,井上,金田：ネットワーク上での情報統合に対するプライバシー保護,情報処理学会論文誌,Vol.41,No.11
[7] 電子コンテンツの利用をセキュアに：日経インターネットテクノロジー2001 年 12 月号